REMARKS

STATUS SUMMARY

Claims 1-15 and 17-27 are pending in the present application. The Examiner has rejected claims 1-15 and 17-27 under 35 U.S.C. § 102(e) as anticipated by U.S. Patent No. 6,763,363 to *Driscoll* ("*Driscoll*").

These formal matters identified in the Office Action are addressed herein below.

RESPONSE TO CLAIM REJECTIONS UNDER 35 U.S.C. § 102(e)

Claims 1-15 and 17-27 are again rejected under 35 U.S.C. § 102(e) as anticipated by *Driscoll*. Applicant respectfully traverses this rejection because *Driscoll* fails to teach each and every feature or element recited in the rejected claims.

First, *Driscoll* is related generally to "private-key stream cipher cryptosystems, which employ linear feedback shift registers to produce pseudo-random bit keystreams, such as keystreams for combining with plaintext to encrypt the plaintext into ciphertext and keystreams for combining with the ciphertext to decipher the ciphertext into plaintext. ... In particular, cryptosystems perform cryptography to transform plaintext into ciphertext so that only an authorized receiver can transform the ciphertext back into the original plaintext." Col. 1: lines 6-13 and 20-23.

In contrast, the claimed invention also is related generally to encryption but in particular, to data encryption of digital data in memory of a digital device. *See specification*, page 1, **[002]**, lines 1-2. Specifically, the claimed invention "provide[s] data encryption and decryption at the

memory interface in a digital device." *See specification*, page 2, **[007]**, lines 1-2. In other words, an object of the invention is to protect unencrypted digital data stored in unsecure rewriteable memory of a digital device or that is encrypted with hard-wired keys that may be vulnerable to reverse engineering. *See specification*, pages 1-2, **[005]**, lines 5-8.

Accordingly, claim 1, as amended, of the present application, as amended, recites the following:

> A system of digital data encryption in a digital device, comprising:
> an encryption key generator;
> a data buffer;
> an input/output register that interfaces with memory of the digital device; and
> a memory controller that directs digital data from the memory to the data buffer with the digital data passing through the encryption key generator prior to entering the input/output register.

As noted above, *Driscoll* is related to linear feedback shift registers ("LFSRs") utilized in private-key cryptosystems while the claimed invention includes systems and methods for data encryption and decryption at the memory interface in digital devices. Thus, *Driscoll* fails to teach or suggest several features or elements recited in the rejected claims.

The first of these features or elements of claim 1 is a data buffer into which the memory controller directs data to be encrypted or decrypted. "Digital data ready for encryption is stored in the data buffer 106." *See specification*, page 4, **[020]**, line 1. "For decryption, the reverse process occurs and the encrypted digital data is decrypted as it is transferred from memory to the I/O register 108 for use via the data buffer 106 by the encryption circuit 102." *See specification*, page 5, **[022]**.

The Examiner refers to col. 7: lines 61-67 and col. 8: lines 1-5 of *Driscoll* as disclosing a data buffer. Looking at this portion of *Driscoll*, however, it is apparent that this portion refers to

into w words of word length M represented as LFSR 0, LFSR 1, ..., LFSR(w-1). Col. 7: 25-32. These storage elements do not constitute a data buffer that stores digital data to be encrypted or decrypted as claimed by claim 1.

As for the second feature or element, an input/output register, the Examiner cites FIGs. 1 and 2 of *Driscoll*, which are block diagrams of a private-key stream cipher cryptosystem according to the invention claimed in *Driscoll* and a sender or receiver in such a cryptosystem, respectively. Col. 4: 53-57. These block diagrams not having any elements described as input or output registers, the Examiner has failed to provide any analysis to show that *Driscoll* teaches or suggests anything regarding an input/output register that receives encrypted data from the encryption circuit prior to being written to memory or from memory prior to being transmitted to the encryption circuit for decryption. *See specification*, page 4, **[004]**, lines 3-5, and page 5, **[022]**.

Finally, *Driscoll* also fails to teach or suggest "a memory controller that directs digital data to the data buffer with the digital data passing through the encryption key generator prior to entering the input/output register." In general, as its title indicates, *Driscoll* teaches "a computer efficient linear feedback shift register." With regard to the memory controller of claim 1 of the pending application, the Examiner cites col. 4: lines 30-46 of *Driscoll*:

> One form of a stream cipher cryptosystem according to the present invention includes a PRNG receiving a key and providing a keystream. The PRNG includes a word-by-word shifting LFSR according to the present invention for providing a LFSR output word of word length M. The stream cipher cryptosystem also includes a cryptographic combiner to provide a second binary data sequence. In encryption operations, the cryptographic combiner is an encryption combiner and the first binary data sequence is a plaintext binary data sequence and the second binary data sequence is a ciphertext binary data sequence. In decryption operations, the cryptographic combiner is a decryption

combiner and the first binary data sequence is a ciphertext binary data numbers sequence and the second binary data sequence is a plaintext binary data sequence.

In general, what *Driscoll* teaches can be best summarized by its FIGs. 3 and 4. FIG. 3 illustrates a conventional bit-by-bit LFSR (col. 6: 48-49) while FIG. 4 generally illustrates a word-by-word left shifting LFSR according to the invention of *Driscoll*. (col. 7: 25-260) with the advantages of the latter LFSR described at col. 9: 14-52. Thus, in summary, all that *Driscoll* teaches is an improved, computer efficient, LFSR. *Driscoll* in fact has no need of a memory controller because it is not related to encryption and decryption of digital data entering and leaving memory of a digital device but to encryption and decryption of ciphertext streams that are transmitted from one computer system to another.

Independent claim 9, as amended, is a claim that includes "a memory controller that sends a memory request," and independent claim 25, as amended, recites a set-top box apparatus that includes "a memory controller that directs the storage of the digital data in the rewritable memory." Independent method claim 12 includes the step of encrypting digital data using a key while the digital data is being placed in a rewritable memory and independent method claim 22 includes the step of generating a memory request to retrieve encrypted digital data.

Thus these remaining independent claims 9, 12, 22, and 25 each include similar limitations as found in claim 1 and these claims are therefore also patently distinct from *Driscoll* for at least the same reasons. In general, that limitation is a memory controller capable of generating a memory control signal that is used to write digital data to rewriteable memory after that digital data is encrypted in an encryption circuit, and that limitation is not taught by *Driscoll*. *Driscoll* therefore fails to teach each and every feature or element recited in each of independent claims 1, 9, 12, 22, and 25.

Driscoll therefore fails to teach each and every feature or element recited in each of independent claims 1, 9, 12, 22, and 25.

Accordingly, Applicant believes that independent claims 1, 9, 12, 22, and 25 are in condition for allowance and because all other claims are dependent directly or indirectly from allowable claims 1, 9, 12, 22, and 25, Applicant respectfully requests that the Examiner withdraw the rejection of claims 1-27 under 35 U.S.C. § 102(e).

CLAIM AMENDMENTS

Amendments have been made to claims 1, 3, 4, 7-9, 10, 13, 18, 22, 25, and 27, to clarify the claimed invention, to improve grammar and readability, and to correct a lack of antecedent basis in certain claims. For example, claims 4, 10, 13, and 18 have been amended to clarify the "key" referred to therein. Claims 25 and 27 have been amended to clarify the antecedent basis with respect to the digital data referred to therein.

Claims 1, 9, and 22 have been amended to clarify that the digital data is stored in memory of a digital device. Support for these amendments may be found, for example, at page 4, paragraph **[019]**, lines 1-3, page 4, paragraph **[021]**, lines 1-2, and page 5, paragraph **[022]**, lines 1-3, and elsewhere throughout the specification. Claims 7 and 8 have been amended to clarify that the key referred to is a key selected from a key store. Support for these amendments may be found, for example, at page 5, paragraph **[023]**, lines 1-6, and page 5, paragraph **[024]**, lines 1-3, FIG. 2, and elsewhere throughout the specification.

None of the amendments to the claims discussed in this section have been made in response to a substantive rejection or for any other purpose relating to patentability, and the

originally filed. Accordingly, no new matter is believed to have been added by these amendments.

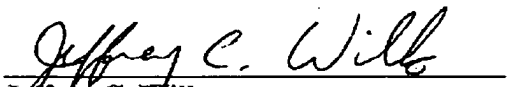
CONCLUSION

In light of the above amendments and remarks, it is respectfully submitted that the present application is now in proper condition for allowance, and an early notice to such effect is earnestly solicited.

If any small matter should remain outstanding after the Patent Examiner has had an opportunity to review the above Remarks, the Patent Examiner is respectfully requested to telephone the undersigned patent attorney in order to resolve these matters and avoid the issuance of another Official Action.

Respectfully submitted,
Winefred Washington

Dated: December 27, 2007

By: 

Jeffrey C. Wilk
Registration No. 42,227
Phone: (818) 488-8148
Fax: (949) 608-3645

The Eclipse Group LLP
10605 Balboa Blvd., Suite 300
Granada Hills, CA 91344